UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,809	12/11/2000	Messaoud Benantar	AUS9-2000-0799-US1	2057

7590 03/09/2005

Joseph R. Burwell
Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, TX 78755-8022

EXAMINER	
ARANI, TAGHI T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/734,809	**Applicant(s)** BENANTAR, MESSAOUD	
	Examiner Taghi T. Arani	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 October 0204*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *5/21/2001* is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-32 have been examined and are pending.

Response to Arguments

2. In view of Applicant's arguments filed 10/21/2004 a new ground(s) of rejection is presented in this Office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1-32** are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al, hereinafter, Van Oorschot (USP 5,699,431) in view of Micali (USP 5,960,083).

As per claims 1, 11, and 21, Van Oorschot teaches a method for validating a digital certificate within a data processing system, the method comprising: receiving a digital certificate (col. 1, line 50);

retrieving a certificate revocation list (col. 1, line 61-62);

extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority (col. 2, lines 7-8);

determining whether the first serial number matches a second serial number stored (col. 2, line 8) within the certificate revocation list. Van Oorschot teaches that a match in the serial number means that the certificate has been revoked. Van Oorschot teaches that in the certificate is option information that specifies where additional access information about certificate may be found (col. 2, lines 56-63). One type of additional access information as disclosed by Van Oorschot is the particular CA that was used to certify that particular certificate (col. 5, lines 13-24). Van Borscht's system can be applied to the X.509 standard of digital certificates. Here is the format of a X.509 certificate.

Van Oorschot fails to teach computing a first certificate fingerprint for the digital certificate and comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

However, Micali teaches computing a first certificate fingerprint for the digital certificate [co. 4, lines 46-67] and comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number [col. 5, lines 22-36, col. 6, lines 26-27, i.e. returning hashed (digital fingerer print) YES-value and NO-value].

It would have been obvious to one of ordinary skill in the art at the time the invention to utilize Micali's method of managing the certificate fingerprint stored within the CRL in Van Oorschot's management of certificate revocation lists in order to facilitate management of public key certificate revocation without providing users of with lists of certificate [Micali, col. 3, lines 6-9].

As per claims 7, 17, and 27, Van Oorschot teaches receiving a serial number for a digital certificate, wherein the serial number has been associated with the digital certificate by a certifying authority (Col. 2, lines 6-8); creating an entry in a certificate revocation list for the digital certificate (Col. 1, lines 50-60), wherein the entry comprises the serial number for the digital certificate (Col. 2, lines 7-8);

Van Oorschot fails to teach computing a certificate fingerprint for the digital certificate and storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate.

Micali teaches computing a certificate fingerprint for the digital certificate and storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate [col. 4, lines 40-67].

It would have been obvious to one of ordinary skill in the art at the time the invention to utilize Micali's method of managing the certificate fingerprint stored within the CRL in Van Oorschot's management of certificate revocation lists in order to facilitate management of public key certificate revocation without providing users of with lists of certificate [col. 3, lines 6-9].

As per claims 2-3, 12-13, and 22-23, Van Oorschot as modified teach in response to a determination that the first certificate fingerprint matches the second certificate fingerprint, invalidating the digital certificate [Micali, col. 5, lines 22-36] and in response to a determination that the first certificate fingerprint does not match the second certificate fingerprint, validating the digital certificate [that is YES-value (continues to be valid) and NO-value (certificate is no longer valid)].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Van Oorschot with the Micali's fingerprint certificate to validate or invalidate the certificate correctly in case a user queries –by error, malice or other reason- the directory about a serial number that does not belong to any not-yet expired certificate [col. 8, lines 1-14 of Micali) issued by a given CA.

As per claims 4, 8, 14, 18, 24, and 28, Van Oorschot teaches the digital certificate and the certificate revocation list are formatted according to the X.509 standard (col. 1, lines 49-67].

As per claims 5, 9, 15, 19, 25, and 29, Van Oorschot as modified teaches the second certificate fingerprint is stored within an X.509 extension within the certificate revocation list (col.4, lines 46, col. 5, lines 1 (CRS)).

As per claim 6, 10, 16, 20, 26, and 30, Van Oorschot as modified teaches the step of computing a first certificate fingerprint for the digital certificate uses a digest algorithm in accordance with a digest algorithm identifier stored in association with the second certificate fingerprint (Micali, col. 4, lines 55-67, see also Van Orchard, col. 5, lines 38-41). Also X.509 standard includes this algorithm identifier field.

As per claims 31 and 32, Van Oorschot teaches a data structure representing a certificate revocation list for use in a data processing system, the data structure comprising: a serial numbers of a revoked digital certificates (col. 2, lines 1-8 and col. 1, lines 49-51). The examiner supplies the same rational for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Micali within the system of Van Oorschot to utilize Micali's method of managing the certificate fingerprint stored within the CRL.

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T.A.
Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100